CLAIMS

1. A method of securely transferring first and second data from a user to first and second parties respectively, wherein:

- the user encrypts the first data using a first encryption key associated with the first party, and then encrypts the second data using, as encryption parameters, both public data of said first party and third data comprising the encrypted first data;
- the third data is provided to the first party and the encrypted second data is provided to the second party;
- the first party uses a first decryption key to decrypt the encrypted first data, as provided to the first party in said third data, whereby to recover the first data; the first party also using the third data, along with private data related to said public data, to generate a second decryption key;
- the second decryption key is provided to the second party which uses it to decrypt the encrypted second data.

2. A method according to claim 1, wherein the first encryption key corresponds to a public key associated with the first party and for which that party has a corresponding private key that constitutes said first decryption key.

3. A method according to claim 1, wherein the first encryption key and the first decryption key are the same.

4. A method according to claim 1, wherein the first data comprises a message with interpretable content.

5. A method according to claim 4, wherein said message comprises an instruction to the first party to carry out a specific action, the first party interpreting the recovered first data and carrying out said specific action.

6. A method according to claim 4, wherein said message comprises a condition to be satisfied before the second decryption key is provided to the second party, the first party interpreting the recovered first data and ensuring that said condition is satisfied before it generates said second decryption key and/or provides that key to the second party.

7. A method according to claim 4, wherein the third data further comprises at least one of a random number and a time indication.

8. A method according to claim 4, wherein the user sends the encrypted second data, together with the third data, to the second party; the second party providing the third data to the first party.

9. A computer system comprising first, second and third computing entities, wherein:

- the first computing entity comprises a first arrangement for encrypting a first data set using a first encryption key associated with a third party; a second arrangement for encrypting a second data set using, as encryption parameters, both public data of said third party and a third data set comprising the encrypted first data set; and a third arrangement for outputting the encrypted second data set for provision to the second computing entity and for outputting the third data set for provision to the third computing entity; and
- the third computing entity is associated with said third party and is arranged to use a first decryption key to decrypt the encrypted first data as provided to the third computing entity in said third data set whereby to recover the first data set; the third computing entity being further arranged to generate, using the third data set and private data related to said public data, a second decryption key for enabling the second computing entity to decrypt the encrypted second data set.

10. A computer system according to claim 9, wherein the first encryption key corresponds to a public key associated with the third party and for which that party has a corresponding private key that constitutes said first decryption key.

11. A computer system according to claim 9, wherein the first encryption key and the first decryption key are the same.

12. A computer system according to claim 9, wherein the first data set comprises a message with interpretable content, the third computing entity being arranged to interpret the content of the recovered first data set.

13. A computer system according to claim 12, wherein said message comprises an instruction to the third computing entity to carry out a specific action, the third computing entity being arranged to interpret the recovered first data set and carry out said specific action.

14. A computer system according to claim 12, wherein said message comprises a condition to be satisfied before the said decryption key is provided to the second computing entity, the third computing entity being arranged to interpret the recovered first data set and ensure that said condition is satisfied before it generates said decryption key and/or provides that key to the second computing entity.

15. A computer system according to claim 12, wherein the third data set further comprises at least one of a random number and a time indication.

16. A computer system according to claim 12, wherein the said third arrangement of the first computing entity is arranged to send the encrypted second data set, together with the third data set, to the second computing entity; the second computing entity being arranged to provide the third data set to the third computing entity.

17. Apparatus comprising:

- first means for forming a first data set comprising a message intended for a trusted authority;

- second means for encrypting the first data set using an encryption key associated with the trusted authority;
- third means for encrypting a second data set using, as encryption parameters, both public data of the trusted authority and a third data set comprising the encrypted first data set;
- fourth means for outputting the encrypted second data set for provision to another party and for outputting the third data set for provision to the trusted authority.

18. Apparatus according to claim 17, wherein said message comprises an instruction to the trusted authority to carry out a specific action.

19. Apparatus according to claim 17, wherein said message comprises a condition to be checked by the trusted authority as being satisfied before the trusted authority provides a decryption key to the said another party for use in decrypting the encrypted second data set.

20. Apparatus according to claim 17, wherein the third data set further comprises at least one of a random number and a time indication.

21. Apparatus according to claim 17, wherein the fourth means is arranged to send the third data set, together with the encrypted second data set, to said another party for the latter to provide the third data set to the trusted authority.

22. A computer program product arranged to condition computing apparatus, when installed thereon, to provide:

- first means for forming a first data set comprising a message intended for a trusted authority;
- second means for encrypting the first data set using an encryption key associated with the trusted authority;

- third means for encrypting a second data set using, as encryption parameters, both public data of the trusted authority and a third data set comprising the encrypted first data set;
- fourth means for outputting the encrypted second data set for provision to another party and for outputting the third data set for provision to the trusted authority.